UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	S1 23 Cr. 430 (KPF)
ROMAN STORM,	:	
Defendant.	:	

OPPOSITION OF THE UNITED STATES OF AMERICA TO THE MOTIONS *IN LIMINE* OF ROMAN STORM

JAY CLAYTON
United States Attorney
Southern District of New York

Ben Arad
Benjamin A. Gianforti
Thane Rehn
Assistant United States Attorneys

Kevin Mosley
Special Assistant United States Attorney
- *Of Counsel* -

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

The Government submits this memorandum in opposition to defendant Roman Storm's motions *in limine*. (Dkt. 155). For the reasons discussed below, the defendant's motions should be denied.

ARGUMENT

I. Opposition to MIL Nos. 1 and 3: The Government Does Not Intend to Offer Evidence or Argument Related to North Korea's Military, Including Its Weapons and Nuclear Missile Programs, Except to the Extent that the Defendant Understood that Funds Stolen by the Lazarus Group Would Be Put to Such Uses and to Provide Necessary Context for Count Three.

Because MILs Nos. 1 and 3 cover similar ground, they are both addressed herein. With respect to MIL No. 1, the defendant argues that the Court should preclude the Government from making any reference, in evidence or argument, to the state-sponsored North Korean cybercriminal group known as the Lazarus Group. The defendant argues that any such evidence or argument should be precluded because "(1) the government has produced no evidence supporting the contention that the Ronin hack was conducted by the Lazarus Group …; and (2) in any event, the identity of the Lazarus Group, and particularly its association with North Korea, is not relevant to the charges here and is substantially more prejudicial than probative." (Dkt. 155 at 3). Accordingly, the defendant contends, this evidence is irrelevant under Rules 401 and 402 and unfairly prejudicial under Rule 403. As discussed below, these arguments fail.

A. Evidence Regarding the Lazarus Group Is Relevant and Admissible Because the Defendant Believed that the Lazarus Group Was Responsible for the Ronin Hack and that the Hacked Funds Might Be Used for North Korea's WMD Program, Evidencing His *Mens Rea*.

Whether the Lazarus Group in fact carried out the Ronin Hack, and whether North Korea used the funds drained from the Ronin bridge to finance its military or weapons-of-mass-destruction ("WMD") program, are beside the point. What is relevant is that the defendant and his Tornado Cash cofounders, Roman Semenov and Alexey Pertsev, *believed* that the Lazarus Group

carried out the hack and that the stolen funds would be used to support North Korea's WMD program, yet chose to continue to provide services to the Lazarus Group, and the sanctioned wallet that they believed to be controlled by the Lazarus Group, by facilitating laundering its ill-gotten gains through the Tornado Cash service. This demonstrates their *mens rea*—both their knowledge of their involvement in transactions that constituted both money laundering and sanctions violations and their willfulness with respect to their participation in these criminal transactions—as to all three counts charged in the Superseding Indictment. Therefore, evidence and argument with respect to the Lazarus Group are relevant and appropriately heard by the jury insofar as the evidence bears on the defendant's state of mind and intent.

The evidence at trial with respect to the Ronin Hack and the Lazarus Group will consist principally of the following: (i) testimony from a representative of the Ronin Network, along with certain business records from the Ronin Network, which will show that there was an unauthorized network exploit in March 2022, resulting in hundreds of millions of dollars' worth of ETH being drained from the Ronin bridge, a blockchain that facilitated play of the blockchain-based video game, Axie Infinity; (ii) expert cryptocurrency tracing analysis from FBI Special Agent Joel DeCapua showing that the majority of these stolen funds went into a particular wallet and from there into the Tornado Cash service in thousands of deposits conducted over a period of more than six weeks; (iii) testimony from a representative of the Office of Foreign Asset Control ("OFAC") that OFAC announced sanctions on this wallet on April 14, 2022, pursuant to its already-existing sanctions on the Lazarus Group (the "Lazarus Group Wallet"); and (iv) the defendant's own numerous statements in his long-running Telegram chat with Roman Semenov and Pertsev (the "Founders Chat"), discussing the Ronin Hack, the OFAC sanctions, and the Lazarus Group.

None of this evidence involves introducing extraneous evidence about the Lazarus Group

or the nature of its relationship with North Korea. Aside from the defendant's own statements, the only anticipated reference to the Lazarus Group will be the OFAC witness who will testify that the sanctions imposed on April 14, 2022, were an implementation of the existing sanctions on the Lazarus Group, testimony that is necessary both to establish an element of the offense—that there were in fact sanctions in place—and to place the defendant's statements in context.

To the extent that there will be any more detailed evidence regarding the Lazarus Group, it will be taken from the Founders Chat. In their messages, the defendant and his co-conspirators circulated multiple online articles attributing the Ronin Hack to the Lazarus Group and discussed this fact. Some of these articles also confirmed that the defendant knew his business was moving money for the Lazarus Group and that his at best half-hearted attempt to block the sanctioned Lazarus Group Wallet from the Tornado Cash service was indeed, as the defendant characterized it, "easy to evade." (Ind. ¶ 64). For example:

- On April 14, 2022, the day that OFAC sanctioned the Lazarus Group Wallet, the defendant sent the link below to Semenov and Pertsev, in which the Ronin Hack was attributed to the Lazarus Group. The defendant noted in response to the link, among other things, as translated from Russian, "guys, we are fucked," "[g]uys, basically, I think this is serious and we need to act very fast," and "[t]he address has already been added to the OFAC list – these hackers are using Tornado. We urgently need to tell everyone that we do not let such individuals to [*sic*] the front" (the front likely being a reference to the Tornado Cash "frontend" or user interface ("UI")). The article sent by the defendant referred to the Lazarus Group as "a criminal group with strong ties to North Korea,…suspected of being behind infamous cyberattacks including the WannaCry ransomware that impacted a wide number of industries and manufacturing, as well as legislative and judicial systems." https://x.com/web3isgreat/status/1514678143793209357

- On April 15, 2022, the defendant sent another link to Semenov and Pertsev, in which the Ronin Hack was attributed to the Lazarus group. The article referred to the Lazarus Group as, among other things, a "hacking outfit[]…associated with North Korea….that…generate[s] revenue for the North Korean regime." The defendant noted in response to the link, among other things, as translated from Russian, "[t]his is very serious," "[g]uys, this is not a joke," and "[a] guy got five years of prison for sanctions." https://time.com/6167383/axie-cryptocurrency-

north-korea-hackers/.

- Just a few minutes later, the defendant sent Semenov and Pertsev a link to a Twitter post that read, in substantial part, "@TornadoCash laundered 26,300 Ether ($72.9 million) for the North Korean government over the last two weeks. Every holder of $TORN is an accomplice to violating sanctions. All Ether held in, or withdrawn from, @TornadoCash wallets is sanctionable." The link to this post is no longer active, but the text of the post is replicated in the Telegram chat's text, which the Government will seek to introduce at trial. In response to the link, the defendant stated, among other things, as translated from Russian, "Shit!"

- On April 16, 2022, the defendant sent the link below about the Ronin Hack to Semenov and Pertsev, which stated, among other things, that "[t]he blacklisted address that U.S. authorities say is controlled by North Korea's elite 'Lazarus' hacker group sent 2,915 ETH (around $8.8 million) to the cleaners this morning New York time, a day after federal officials listed it on its sanctions database. Making a brief pit stop at a fresh, unsanctioned wallet, its crypto quickly flew through the popular coin mixer Tornado Cash, where the trail went cold." In response, Semenov stated, among other things, as translated from Russian, "ultimately Chainalysis Oracle is to blame for everything because they are too slow at adding addresses." The defendant replied to Semenov as follows, "[n]ot them but OFAC" and "Chainalysis adds them quite fast." https://www.coindesk.com/tech/2022/04/15/sanctioned-crypto-wallet-linked-to-north-korean-hackers-keeps-on-laundering.

- On May 6, 2022, the defendant forwarded to Semenov and Pertserv what appears to be a headline from an article reading, "U.S. Authorities sanction the Blender.io mixer. Sanctions were also imposed on addresses associated with the mixer. Blender.io is allegedly linked to North Korean hackers. ☝ It is the first time when the U.S. Treasury has added a cryptocurrency mixer to its sanctions list." The defendant then stated, among other things, as translated from Russian, "[h]ow about that? That went through Tornado as well," an apparent acknowledgment that other funds tied to North Korea were also laundered through Tornado Cash.

- About an hour later, Semenov sent the link below to a U.S. Treasury press release to the defendant and Pertsev, which stated, among other things, that "On March 23, 2022, Lazarus Group, a [North Korean] state-sponsored cyber hacking group, carried out the largest virtual currency heist to date, worth almost $620 million, from a blockchain project linked to the online game Axie Infinity…. Under the pressure of robust U.S. and UN sanctions, [North Korea] has resorted to illicit activities, including cyber-enabled heists from cryptocurrency exchanges and financial institutions, to generate revenue for its unlawful weapons of mass destruction (WMD) and ballistic missile programs." In response, the defendant added an up arrow—"^"—indicating the U.S. Treasury press release was about the same thing that the defendant had messaged his co-founders about earlier.

https://home.treasury.gov/news/press-releases/jy0768.[1]

The messages surrounding these links reflect that the defendant and his co-conspirators believed that the Lazarus Group—a known cybercriminal group—was responsible for the Ronin Hack and that the Lazarus Group was laundering the proceeds of that hack through the Tornado Cash service so that they could be put to nefarious purposes, including North Korea's WMD program. Indeed, the defendant and his co-conspirators openly shared this information with each other, referenced the specific sanctions that these transactions violated, and discussed their potential criminal liability for their ongoing facilitation of transactions with the Lazarus Group, evidencing their knowledge, their willfulness, and their consciousness of guilt. But the defendant and the other founders continued to facilitate these transactions, thereby committing sanctions violations themselves, and declined to take steps to prevent the transactions, which also evinces their willfulness with respect to these violations. Accordingly, these and other references to the Lazarus Group and the potential uses of its stolen funds—which, again, are embedded in or linked to by statements made by the defendant and his co-conspirators—are relevant and should be presented to the jury as evidence of the defendant's *mens rea*. *See United States v. Hassan*, 578 F.3d 108, 128 (for purposes of conspiracy to commit money laundering charge, evidence was sufficient to show that defendant "believed that the funds related to" unlawful activity where defendant had been present at another person's bond hearing where attorneys referenced the unlawful activity and had an "encounter" with a law enforcement agent who told him about the

[1] The defendant's Google internet browsing history, which the Government also will seek to introduce at trial, also demonstrates his knowledge and belief that the Lazarus Group committed the Ronin Hack and laundered the proceeds through the Tornado Cash service, as he visited multiple sites that published articles to this effect during the same time period. In addition, on April 15, 2022, the defendant googled, "tornado cash north korea."

unlawful activity).

Nor are the links that the defendant and his co-conspirators shared in the Founders Chat inadmissible hearsay.

First, the Government would not be offering the links circulated in the Founders Chat for the truth of the matters they assert, so they are not hearsay at all. Fed. R. Evid. 801(c). As the defendant correctly notes, the Government need not prove the identity of the perpetrator of the Ronin Hack or the potential uses of the funds stolen in the hack to convict the defendant of any of the Government's charges. (Dkt. 155 at 7). But proof of the defendant's *understanding* of the identity of the perpetrator of the Ronin Hack and how the stolen funds might be put to use is nonetheless relevant to demonstrate the defendant's *mens rea* and thus is admissible, non-hearsay evidence. And the Court could issue an appropriate limiting instruction to that effect. *See, e.g.*, *United States v. Bell*, 112 F.4th 1318, 1340–41 (11th Cir. 2024) (affirming district court's admission, with a limiting instruction, of media reports and press releases about fraudulent schemes similar to the one charged that were shared via email among co-conspirators as "proof that the [co-conspirators] were on notice of the wrongfulness of their conduct and of the fact that other individuals had been prosecuted for similar behavior"); *see also Hassan*, 578 F.3d at 128 (discussing evidence of what money laundering conspiracy defendant had learned in "encounter with" law enforcement agent). As in *Bell*, the various links circulated among the Tornado Cash founders—particularly those sent by the defendant himself—are proof that the defendant and his co-conspirators were on notice of, among other things, the wrongfulness of their actions in facilitating transactions derived from the Lazarus Group's unlawful conduct and that others had been prosecuted for similar conduct. Indeed, as the defendant noted in the Founders Chat on April 15, 2022, as translated from Russian, "[a] guy got five years of prison for sanctions."

Second, the links that the defendant and his co-conspirators shared with each other in the Founders Chat are also not hearsay because they would be "offered against an opposing party…[who] manifested that [he] adopted or believed [them] to be true." Fed. R. Evid. 801(d)(2)(B). As noted above, the defendant and his co-conspirators' reaction to the various links attributing the Ronin Hack to the Lazarus Group and describing the potential uses of the stolen funds was concern about their criminal exposure because they believed what they had read. At no point did they express doubt about the veracity of the contents of the articles they circulated.

In *United States v. Ho*, 984 F.3d 191 (2d Cir. 2020), a prosecution under the Foreign Corrupt Practices Act, the defendant traveled to Chad as part of an entourage representing a Chinese energy conglomerate that was trying to do business there. During a meeting with the Chadian president, the entourage presented the president with wrapped gift boxes containing $2 million in cash. *Id*. at 196. The president was not pleased and summoned the entourage, including the defendant, back to his compound the following day. *Id*. At that meeting, the president "expressed shock and anger at receiving cash, and explained that he did not know 'why people believe all African leaders are corrupt.'" *Id*. (quoting trial transcript). In response, the defendant stated that "he was 'very impressed by [the president's] reaction and…attitude.'" (*Id*.) (editing and quotation marks in original) (quoting trial transcript). The district court admitted the Chadian president's statement under Rule 801(d)(2)(B). The Second Circuit found no abuse of discretion and affirmed, noting, among other things, that the defendant did not "[dis]agree with [the Chadian president's] representation [about the attempted cash bribes] or [state that he (the defendant)] had not been aware of the alleged cash bribes," because the circumstances indicated that the defendant "would have said so" if he did disagree or had not been aware of the attempted bribes. *Id*. at 207-08 (citing *United States v. Guzman*, 754 F.2d 482, 487 (2d Cir. 1985); *United States v. Shulman*,

624 F.2d 384, 390 (2d Cir. 1980); *United States v. King*, 560 F.2d 122, 134–35 (2d Cir. 1977)); *see also Pietrangelo v. Refresh Club, Inc.*, No. 18-CV-1943 (DLF), 2023 WL 6388880, at *11 (D.D.C. Sept. 29, 2023) (admitting under Rule 801(d)(2)(B) defendant co-working space's "retweets" of "various news publications' statements characterizing [defendant co-working space] as a 'women's-only' organization" in gender discrimination case based on defendant co-working space's "'unambiguous[] assent[]' to the news-publication tweets") (quoting *United States ex rel. Landis v. Tailwind Sports Corp.*, 292 F. Supp. 3d 211, 221 (D.D.C. 2017)).

The same logic applies here. If the defendant and his co-conspirators did not believe what they read in the various links they circulated attributing the Ronin Hack to the Lazarus Group and reporting that the Lazarus Group was laundering the stolen funds through the Tornado Cash service, the Founders Chat would reflect that disbelief. But there is no such evidence, indeed, their own statements show exactly the opposite. As such, the Founders Chat is powerful evidence of their willfulness with respect to sanctions violations. Accordingly, the links in the Founders Chat—particularly those the defendant circulated—are admissible as non-hearsay evidence of his *mens rea* under Rule 801(d)(2)(B).

B. Evidence Regarding the Lazarus Group Is Also Relevant and Admissible Because It Is Necessary Context for Count Three.

As the Government noted in a letter to the defense dated February 18, 2025, the Government intends to call John Pisa-Relli, an OFAC employee, who will testify about OFAC's general function and that, based on his review of OFAC records, in September 2019, OFAC designated the Lazarus Group for sanctions based on its relationship to North Korea's primary intelligence bureau. Pisa-Relli will also testify that, on April 14, 2022, OFAC designated as blocked property of the Lazarus Group the Lazarus Group Wallet, which is an ETH wallet address

beginning with the characters 0x098B716. Pisa-Relli will further testify that the following individuals and entities did not obtain licenses to conduct any transactions with or services for the Lazarus Group or the Lazarus Group Wallet: the defendant, Semenov, Pertsev, Tornado Cash, and Peppersec, Inc., the Delaware corporation co-owned by the defendant and the other Tornado Cash founders under which the Tornado Cash service was developed, marketed, and maintained. This testimony is essential to prove the elements of Count Three, which requires the Government to establish the existence of the sanctions that were violated—either the general sanctions on the Lazarus Group (as an agency, instrumentality, or controlled entity of the Government of North Korea) or the specific designation of the Lazarus Group Wallet pursuant to those sanctions—and that the defendant was not licensed to transact with the Lazarus Group or the Lazarus Group Wallet. For this reason, such evidence is relevant and therefore admissible. Fed. R. Evid. 401, 402.[2]

C. The Government's Proposed Evidence and Argument With Respect to the Lazarus Group Does Not Pose A Rule 403 Problem, Particularly If Accompanied by an Appropriate Limiting Instruction.

Evidence and argument with respect to the Lazarus Group and how it might use criminal proceeds would not run afoul of Rule 403 because it is highly probative of the defendant's *mens rea* as to all three counts (as described above), and it provides necessary background with respect to the sanctions at issue in Count Three. Those qualities are not substantially outweighed by the potential for unfair prejudice. As noted above, the only evidence regarding North Korea's use of hacked cryptocurrency for its military and WMD program that the Government intends to

[2] The defendant's argument about the reliability of Chainalysis's attribution methodology is a red herring (Dkt. 155 at 6) because the Government does not intend to introduce any evidence based on Chainalysis attributions, as the Government has repeatedly reminded the defense.

introduce is evidence that shows what the defendant understood—for example, when he circulated the Treasury Department's press release that referenced North Korea's WMD program in the Founders Chat. Any risk of unfair prejudice would be mitigated by an appropriate limiting instruction that this evidence is being admitted to show the defendant's intent and state of mind, which the Government is happy to work with the defense to draft for the Court's consideration.

The Government does not expect to elicit reference to WMD programs from Pisa-Relli, but it does intend to elicit an explanation that the sanctions on the Lazarus Group were imposed due to the Lazarus Group's ties to North Korea. Relevant evidence "includes background evidence, which can be admitted 'to enable the jury to understand the complete story of the crimes charged.'" *United States v. Ingrao*, No. 23-7687-CR, 2025 WL 1261696, at *5 (2d Cir. May 1, 2025) (quoting *United States v. Reifler*, 446 F.3d 65, 92 (2d Cir. 2006)). In *United States v. McKeeve*, 131 F.3d 1, 13 (1st Cir. 1997), the First Circuit upheld the admissibility of testimony from a Treasury official that the IEEPA embargo against Libya, which the defendant was convicted of violating in connection with shipping computer equipment to Libya, resulted from a presidential determination that Libya supported international terrorism. Specifically, "[t]he government called [the Treasury official] to establish the existence and effect of the economic sanctions imposed against Libya." *Id.* In finding that it was well within the district court's discretion to admit this testimony, the First Circuit noted that the "description of the purpose behind the embargo provided the jury with relevant background information that helped to stitch together an appropriate context in which the jury could assess the evidence introduced during the trial." *Id.* (citing *United States v. Castro–Lara*, 970 F.2d 976, 981 (1st Cir. 1992); *United States v. Daly*, 842 F.2d 1380, 1388 (2d Cir. 1988)).

The logic of *McKeeve* fully applies here, where the defendant is similarly charged with

IEEPA violations for providing a good or service that he claims is otherwise legal to provide, and it is the identity of the counterparty that makes the transaction criminal. Indeed, as the *McKeeve* court noted, "[t]rials are meaty affairs, and appellate courts should not insist that all taste be extracted from a piece of evidence before a jury can chew on it." *Id*. at 13-14. By contrast, the cases upon which the defendant relies—*United States v. Elfgeeh*, 515 F.3d 100 (2d Cir. 2008) and *United States v. Al-Moayad*, 545 F.3d 139 (2d Cir. 2008)—are inapposite. (*See* Dkt. 155 at 10).[3]

In *Elfgeeh*, the defendant went to trial in 2005 in the Eastern District of New York on charges of participating in a conspiracy to operate an unlicensed money transmission business, in violation of 18 U.S.C. §§ 371 and 1960, and of structuring financial transactions, in violation of 31 U.S.C. § 5324(a)(3). At trial, a Special Agent with the Federal Bureau of Investigation referred to terrorism during his testimony. *Elfgeeh*, 515 F.3d at 126-27. The defendant was not on trial for any terrorism-related charges, and, as a result, the district court "promptly gave a curative instruction to the jury, stating that the case was not about terrorism," as well as other "cautionary instruction[s]." *Id*. at 127. In denying the defendant a new trial based on the Special Agent's testimony, the Second Circuit stated that "[t]here can be little doubt that in the wake of the events of September 11, 2001, evidence linking a defendant to terrorism in a trial in which he is not charged with terrorism is likely to cause undue prejudice," but ultimately found that the district court's curative instructions addressed the risk of unfair prejudice under Rule 403. *Id*.

Elfgeeh is distinguishable in two respects. First, the defendant in *Elfgeeh* was not charged

[3] In his third motion *in limine*, which is largely repetitive of his first, the defendant cites just one case, *Doe v. Lima*, No. 14 Civ. 2953 (PAE), 2020 WL 728813, at *6 (S.D.N.Y. Feb. 13, 2020), a civil proceeding under 42 U.S.C. § 1983, in which Judge Engelmayer assessed the admissibility of the plaintiff's prior robbery and sex offenses under Federal Rule of Evidence 609. *Doe* is plainly distinguishable and its relevance here is unclear.

with anything relating to terrorism, whereas the defendant in this case is charged with violating North Korea-related sanctions, of which he was well aware as part of his crimes, making some reference to North Korea necessary in this case. Second, the Second Circuit in *Elfgeeh* was mindful of the uniquely inflammatory nature of references to terrorism in a trial that took place in New York shortly after the events of September 11, 2001. No such unique circumstances are present here. North Korea in 2025 simply does not loom in the public consciousness in the way terrorism did in New York City 20 years ago. And, as already discussed, references to the Lazarus Group by the defendant and his co-conspirators are highly probative of the defendant's *mens rea* and therefore relevant, and such references are otherwise admissible as non-hearsay and necessary context for Count Three. Any potential unfair prejudice can be cured with a limiting instruction to the jury.

The *Al-Moayad* appeal also involved an Eastern District of New York trial that occurred in 2005. *Al-Moayad*, 545 F.3d at 151. There, the defendants were charged with various offenses relating to providing material support to the terrorist organizations Hamas and Al-Qaeda, in violation of 28 U.S.C. § 2339B(a)(1). The testimony at issue in *Al-Moayad* was far more inflammatory than anything the Government is proposing to offer in this case, which will consist principally of testimony from the OFAC representative, victim testimony related to the Ronin Hack (which is not expected to reference the Lazarus Group), and the defendant and his co-conspirators' own statements in the Founders Chat referencing the Lazarus Group. For example, in *Al-Moayad*, the Government called a law student who personally witnessed a bus bombing in Tel Aviv (with which the defendants were not charged) and an individual who had spent time at an Al-Qaeda training camp in Afghanistan. *Id*. at 159. With respect to the law student's testimony, that Second Circuit held that, "given the highly charged and emotional nature of the testimony and

its minimal evidentiary value, the court's decision [to admit the testimony] was arbitrary. The court also refused to give a limiting instruction proposed by the defense, which could have cabined the prejudicial effect of [the law student's] testimony." *Id*. at 160. With respect to the other individual's testimony, the Second Circuit faulted the district court for failing to conduct any Rule 403 analysis as to testimony that went beyond what the Government had represented it would present to include "testimony about the camp, and…the…presentation of images of [Osama] Bin Laden and [Ayman] Al–Zawahiri, [which] was highly inflammatory and irrelevant." *Id*. at 162-63.

Again, the Court should not be blind to the unique historical circumstances of the *Al-Moayab* trial and the particular sensitivities at issue at that time, none of which are present here. Furthermore, nothing that the Government intends to offer at trial will come close to the evidence in *Al-Moayab* that the Second Circuit found crossed the line and was irrelevant. For all these reasons, Rule 403 does not bar reference to the Lazarus Group at trial.[4]

D. The Government Cannot Be Compelled to Stipulate Away Its Evidence with Respect to the Lazarus Group.

The defendant offers "to stipulate that the [Lazarus Group] wallet address was designated as an SDN," which would permit the Government to "simply use the term 'sanctioned entity' without further explication." (Dkt. 155 at 9). But for the reasons detailed above, that stipulation would not adequately correspond to the proof at trial, which, significantly, will include the

[4] Nor does reference to the Lazarus Group run any risk of confusing or misleading the jury, unduly delaying the trial, or wasting anyone's time. (Dkt. 155 at 10-11). All the evidence that the Government intends to introduce with respect to the Lazarus Group is straightforward, particularly the Founders Chat, where the defendant and his co-conspirators circulate incriminating links and then comment on them in plain language. And, as described above, because the relevant issue is what the defendant and his co-conspirators *believed*, there is no need for a "mini-trial" on the reliability of the FBI's or anyone else's attribution of the Ronin Hack to the Lazarus Group or to what uses the funds stolen during that hack might be put. (Dkt. 155 at 11). Those questions are irrelevant.

defendant's own repeated references to the Lazarus Group and its role in the Ronin Hack. Nor would such a stipulation reasonably impart to the jury the defendant's intent and state of mind in choosing to facilitate these particular transactions. This is unlike the unique situation of a prior-conviction element, and thus a stipulation that excises references to the Lazarus Group is not necessary or even workable. *See Old Chief v. United States*, 519 U.S. 172, 186–87 (1997) (acknowledging that the "standard rule that the prosecution is entitled to prove its case by evidence of its own choice, or, more exactly, that a criminal defendant may not stipulate or admit his way out of the full evidentiary force of the case as the Government chooses to present it…is unquestionably true as a general matter").[5]

II. Opposition to MIL No. 2: The Court Should Deny the Defendant's Motion to Preclude the Government from Introducing Victim Testimony or "Referencing Victim Impacts."

In operating the Tornado Cash service, the defendant conspired to launder and transmit cryptocurrency that had been fraudulently obtained or outright stolen from victims. The defendant was well aware that the Tornado Cash service was widely used for these purposes, in part because he repeatedly communicated with his co-conspirators and others about funds from criminal exploits flowing through the service—including proceeds of the Ronin Hack, perpetrated by the sanctioned Lazarus Group. Moreover, when victims contacted the Tornado Cash service directly to seek help, the defendant and his co-conspirators did not lift a finger—except to provide stock responses that falsely claimed there was nothing they could do. The evidence at trial will show

[5] *Old Chief*'s ultimate ruling—that the Government could be compelled to accept a stipulation as to a defendant's commission of a prior felony for purposes of establishing that element of a felon-in-possession of a firearm charge under 18 U.S.C. § 922(g)(1)—is *sui generis*. *Old Chief*, 519 U.S. at 191-92. There is no equivalent element of any of the offenses charged here where a stipulation would prevent the introduction of inherently unfair evidence (like the nature of a prior felony conviction) and therefore *Old Chief*'s specific holding is inapposite.

that there were many victims who lost significant sums of money, traced their stolen funds on the blockchain until the trail went cold at the Tornado Cash service, and contacted the defendant and his co-conspirators to no avail, all of which is directly relevant to the charged conduct, highly probative, and far from unduly prejudicial. Accordingly, the defendant's motion to preclude the Government from introducing victim testimony or "referencing victim impacts" should be denied. (Def. MIL No. 2 at 11).

Victim testimony is highly relevant to—and probative of—each of the charged offenses. As relevant here, Count One of the Indictment requires the Government to prove that the defendant conspired to engage in financial transactions that "involve[d] the proceeds of specified unlawful activity" ("SUA") and that the transactions were "designed in whole or in part . . . to conceal or disguise the . . . location, the source, . . . or the control of" those proceeds. 18 U.S.C. § 1956(a)(1)(B)(i). Much as Count One requires the Government to prove that the funds involved in the transaction actually were the proceeds of an SUA (or because this is a conspiracy charge, that the defendant believed they were derived from an SUA), Count Two requires, among other things, a conspiracy to transmit "funds that are known to the defendant to have been derived from a criminal offense." 18 U.S.C. § 1960(b)(1)(C).

Testimony that victims were deprived of funds by fraud or theft is direct evidence of the existence of the charged SUAs with respect to Count One (here, wire fraud and computer fraud and abuse), the criminal origin of transmitted funds with respect to Count Two, and the defendant's knowledge of the funds' criminal roots with respect to both counts. *See, e.g.*, *United States v. Rahmankulov*, No. 20-CR-653 (RA) Trial Tr. at 117-53 (S.D.N.Y. 2022) (where, as in this case, the Government introduced victim testimony to prove the existence of an SUA that was not perpetrated by the defendant); *United States v. Barton*, 526 F. App'x 360, 363 (5th Cir. 2013)

(finding that evidence was sufficient to prove money laundering charges in part because victim testimony helped establish that certain transfers were obtained by fraud—thus proving the existence of the SUA underlying the money laundering charges); *United States v. Liner*, 435 F.3d 920, 925 (8th Cir. 2006) (finding that evidence was sufficient to prove money laundering charge in part because victim testimony helped establish that the defendant knew he was transacting "in criminally derived property"). Similarly, the testimony of victims who sought assistance from the Tornado Cash service and were ignored or given false, boilerplate responses that the defendant and his co-conspirators were powerless to help establishes that the defendant knew essentially in real time about the commission of the charged SUAs and that criminally-derived funds were flowing through his business—and that his continued concealment and transmission of those funds was willful.

Testimony regarding victim impact—including in the form of loss amounts—is equally relevant to intent because it demonstrates the unique ability of the Tornado Cash service to launder immense sums of cryptocurrency, which underscores the implausibility of any claim that the defendant was unaware his organization was laundering hundreds of millions of dollars' worth of assets. Extensive reporting on the Ronin Hack, published weeks before the Lazarus Group stopped depositing its stolen funds into the Tornado Cash service, revealed that approximately 600 million dollars' worth of cryptocurrency had been stolen. The defendant and his co-conspirators discussed this news the day it broke and shared with each other the Ronin Network's announcement of the hack. Their communications reveal that they quickly deduced from the significant sum of stolen cryptocurrency that the hackers would turn to the Tornado Cash service to conceal their loot. In one communication on March 29, 2022, Semenov wrote to the defendant, as translated from Russian, "Have you seen a $600M hack today? Shit might seriously hit the fan now."

Within days, on April 4, 2022, a journalist had reached out to the defendant about a story she was writing about "the wallet associated with the Ronin hack making Eth deposits to Tornado Cash." After sharing the email with his co-founders, the defendant stated, as translated from Russian, that it was "as if [Semenov] saw it in a crystal ball. It's going to start." In other words, the defendant was noting that Semenov's prediction had come true: the proceeds of the high-profile hack were beginning to flow into the Tornado Cash service and the world was noticing. The co-founders then discussed the ongoing laundering among themselves repeatedly over the ensuing weeks—including in the chats referenced above regarding the Lazarus Group—as the money was being laundered through the Tornado Cash service on an ongoing basis, day in and day out. The Ronin Hack loss amount, of noted significance to the conspiracy, and the manner in which it flowed through the Tornado Cash service for weeks while the defendant was fully aware of this and continued to enable it, is therefore directly probative of the defendant's knowledge that Ronin Hack funds flowed through the Tornado Cash service—and of the defendant's willfulness in continuing to launder and transmit the Lazarus Group's criminal proceeds.

Victim testimony about the Ronin Hack and the losses it caused will demonstrate not only that the defendant willfully laundered funds derived from an SUA and transmitted criminal proceeds through the Tornado Cash service but, with respect to Count Three, that he knowingly transacted with the sanctioned Lazarus Group. *See* 50 U.S.C. § 1705(a), Executive Order 13722, and 31 C.F.R. §§ 510.201 (prohibiting, among other things, knowing transactions with specially designated nationals and blocked persons). What the defendant ultimately saw when he learned that more than half a billion dollars' worth of cryptocurrency might move through the Tornado Cash service was the profit he would reap. Semenov's message to the defendant that "shit might seriously hit the fan" was sent nearly *two months* before the Lazarus Group *stopped* depositing its

criminal proceeds into the Tornado Cash service, two months in which the defendant continued to willfully facilitate these transactions through features of the Tornado Cash service that he controlled, and declined to take steps to stop participating in these criminal transactions. That the defendant and his co-conspirators saw the need to make a public announcement disclaiming responsibility, and did so by implementing a remedy they knew would be ineffective—the Chainalysis sanctions Oracle—to purportedly prevent the Lazarus Group from continuing to launder sanctioned criminal proceeds in those two months, is further evidence of their willfulness. Accordingly, victim testimony regarding the Ronin Hack—including about the loss amount resulting from that hack—should be admitted at trial, whether in the form of victim testimony or otherwise.[6]

The defendant's contention that victim testimony would be unduly prejudicial is unavailing. As set forth above, victim testimony is routine in money laundering cases and especially probative here, given the Tornado Cash service's unique ability to launder money at scale. *Rahmankulov*, No. 20-CR-653 (RA), Trial Tr. at 117-53; *Barton*, 526 F. App'x at 363; *Liner*, 435 F.3d at 925. Indeed, the expected victim testimony in this case bears no resemblance to evidence that courts have found unfairly prejudicial—including in the cases cited by the defendant. (*See* Def. MIL No. 2 at 12-13 (citing *United States v. Hendricks*, 921 F.3d 320, 330 (2d Cir. 2019) (finding that the district court abused its discretion by admitting "testimony regarding [a victim's] fear of groups of black men [because it] carried a substantial risk of evoking racial bias"); *United States v. Paccione*, 949 F.2d 1183, 1201 (2d Cir. 1991) (affirming exclusion of *defense* character

[6] Tellingly, in his bid to stave off probative victim testimony, the defendant does not even attempt to engage with the elements of money laundering, illegal money transmitting, or sanctions evasion. He also fails to cite a single case where a court barred victim testimony—about victim impact or otherwise—as irrelevant to such charges (or charges of conspiring to commit those offenses).

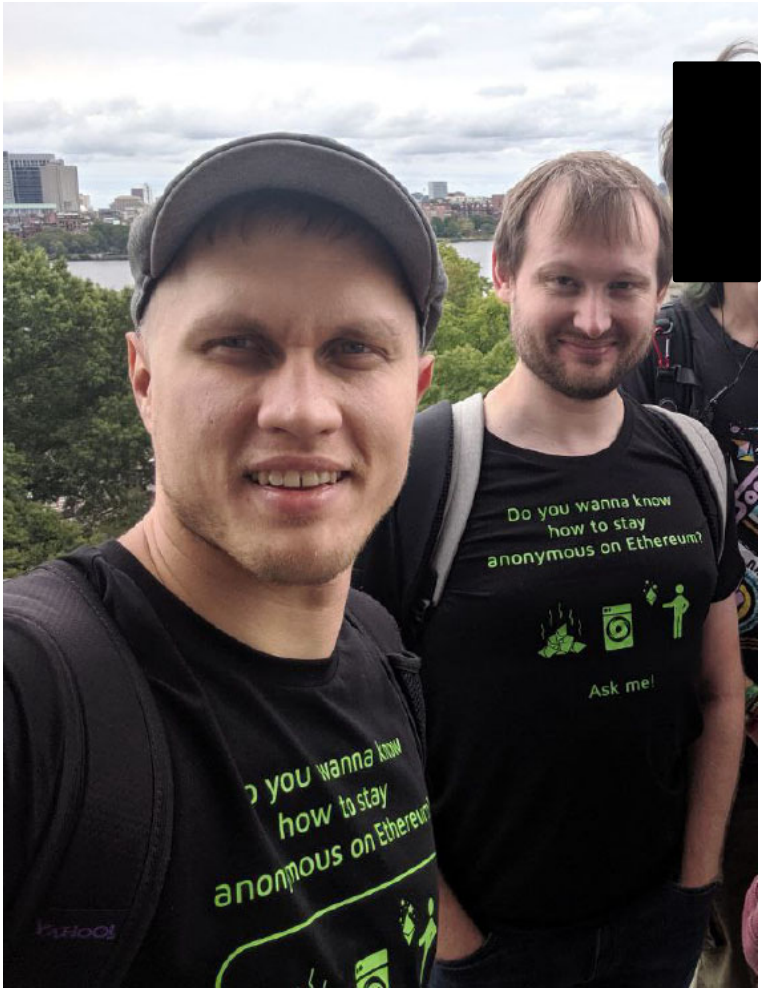
witness testimony regarding the defendant's son's irrelevant illness); *United States v. Malka*, 602 F. Supp. 3d 510, 527 (S.D.N.Y. 2022) (citing *Paccione* and other cases in which sympathy-evoking testimony offered *by the defendant* was inadmissible))).

In sum, the Government should be permitted to introduce victim testimony, including victim impact testimony regarding the losses from the specified unlawful activities whose proceeds were laundered by the Tornado Cash service, because it is not only relevant but highly probative of the charged offenses and carries comparatively little risk of unfair prejudice.

III. Opposition to MIL No. 4: The Defendant Has Asserted No Valid Grounds for Barring the Government from Introducing Evidence or Argument Regarding the Defendant's T-Shirt Featuring a Washing Machine with the Tornado Cash Logo.

At trial, the Government will seek to introduce the following photograph and other documents that depict the image emblazoned on the defendant's t-shirt, which shows the Tornado Cash logo on a washing machine, with a pile of "dirty" ETH symbols on the left, and a "clean" ETH symbol on the right. The Government will also seek to introduce records from a hard drive found in the defendant's house that indicate that the defendant designed the t-shirt himself. The defendant as the individual on the left, and the other individual wearing the t-shirt is Semenov.[7]

[7] The face of third individual depicted here has been redacted to respect his privacy.



The defendant's arguments against admission of this and similar images, though couched in the Rules of Evidence, are, for the most part, factual ones that should be put to the jury, not decided ahead of time in pretrial motion practice. For example, the defendant asserts that these "marketing materials" should be excluded because they are "devoid of any context." (Dkt. 155 at 14). Of course, that is exactly what trials are for: providing context. The defendant is able to provide context for the jury if he chooses to do so.

The defendant also complains that "the government cannot connect any dots to prove that those materials showed any intent or motive regarding Tornado Cash's target market," which should cause the Court to exclude these materials. But, of course, the jury is free to draw whatever

reasonable inferences it wants from these materials, including the obvious one: that a washing machine is about as literal an image for money laundering as one could possibly imagine. The jury is also free to draw the inference that the proof is in the pudding as to the intended target of these marketing materials, as the evidence at trial will show that the Tornado Cash service's customer base ended up consisting in large part of criminals seeking to launder criminal proceeds. Whatever context the defendant might wish to provide for these marketing materials, the Government notes that the t-shirt does not use the word "privacy"—the purported *raison d'être* of the Tornado Cash service—anywhere. It does, however, appear to depict the Tornado Cash service laundering what appears to be a dirty pile of ETH.

Next, the defendant attempts to exclude these images because they are "nothing more than a crude cartoon attempting to simplify and poke fun at its subject matter, and on their face not meant to be taken literally." (Dkt. 155 at 14-15). Again, the defendant is free to argue that he did not mean to be taken literally when he invoked laundering in reference to the Tornado Cash service, but the image plainly does just that, and evidence of how the defendant promoted the service is undoubtedly relevant to his intent.

The defendant also points to the t-shirt's purported use "at an early and reputable Ethereum conference, ETH Boston 2019," as a reason to exclude images of it. (Dkt. 155 at 15). According to the defendant, the t-shirt is irrelevant to the Government's case because it was "only used in or about fall 2019—prior to the time period that any of the charged conspiracies allegedly began." (*Id.*). In support of that proposition, the defendant fails to cite any cases.

As a factual matter, the metadata for the image included above, which was extracted from a hard drive seized from the defendant's home pursuant to a search warrant, indicates that it was created on or about May 28, 2020. The metadata for other, similar images with the washing

machine logo indicate that they were created in late 2020 and even as late as in or about August 2021, well into the charged time period for Count One.

But even setting aside what the metadata indicates for each image, nothing bars the Government from presenting evidence from outside the charged time period for any of the conspiracies alleged in the Superseding Indictment. *See United States v. Reed*, 576 F. App'x 60, 61 (2d Cir. 2014) (affirming district court's admission of "evidence of the charged conspiracy that predated the timeframe alleged in the superseding indictment" because the district court "properly concluded, it 'arose out of the same transaction or series of transactions as the charged offense, is inextricably intertwined with the evidence regarding the charged offense, or is necessary to complete the story of the crime on trial'" (quoting *United States v. Carboni*, 204 F.3d 39, 44 (2d Cir. 2000)) (internal editing omitted). Here, for example, the image included above is relevant and admissible because it plainly arises out of the same series of transactions as the charged offenses (the ownership, development, promotion, and maintenance of the Tornado Cash service); is inextricably intertwined with the evidence of the charged money laundering, unlicensed money transmission, and sanctions evasion conspiracies; and provides crucial context to complete the story of the crime. Indeed, this image (and the others like it) is probative of (at least) the defendant's ownership and promotion of the Tornado Cash service, his conspiracy with Semenov, and their state of mind regarding the Tornado Cash service—namely, that it was designed and promoted as a money laundering tool.

The defendant's argument under Rule 403 fares no better. Here, again, the defendant raises the specter of a "mini-trial on tangential issues." (Dkt. 155 at 16). If the defendant wishes to introduce admissible evidence to try to contextualize this evidence of his intent, he is free to do so. Tellingly, the defendant does not even bother to argue that this evidence is unfairly prejudicial

(and cites no case law at all in this section of his MILs) and for an obvious reason: the evidence is only "prejudicial" because it is probative of the defendant's guilt. *See, e.g.*, *Costantino v. Herzog*, 203 F.3d 164, 174 (2d Cir. 2000) ("Because virtually all evidence is prejudicial to one party or another, to justify exclusion under Rule 403 the prejudice must be unfair.").

IV. Opposition to MIL No. 5: Evidence of the Defendant's Profits from the Tornado Cash Service is Admissible

As the Government argued in its motions *in limine*, the defendant's creation of the TORN token and the distributions to him as a founder and early user of the Tornado Cash service "is evidence of how the service functioned and demonstrates that he did in fact exercise ownership and control of the Tornado Cash service." (Dkt. 157 at 31).[8] This evidence also shows that the defendant had motive to exercise that control in a way that would "increase the value of his TORN holdings." (Dkt. 157 at 31). In addition, that the defendant himself profited from his control of the Tornado Cash service is particularly relevant in establishing an element of the money transmitting offense as it would tend to show that "the Tornado Cash service was an 'enterprise that is carried on for profit or financial gain." (Dkt. 157 at 31 (citing *United States v. Banki*, 685 F.3d 99, 114 (2d Cir. 2012))).

Although evidence admissible as direct evidence is not "subject to consideration under Rule 404(b) at all," *United States v. Halak*, 78 F. App'x 758, 760 (2d Cir. 2003), evidence of the defendant's profits from the sale of his TORN tokens is also admissible under that Rule as "highly probative of the defendant's intent and financial motives in operating the Tornado Cash service," (Dkt. 157 at 31), particularly after he learned that the Tornado Cash service was being used to

[8] The defendant's motions *in limine* do not seek to preclude admission evidence of the defendant's creation and distribution of TORN for these purposes.

facilitate substantial money laundering. (Dkt. 157 at 31-32 (citing cases including *United States v. Motovich*, No. 21 Cr. 497 (WFK), 2024 WL 3303723, at *2 (E.D.N.Y. July 2, 2024) (holding in a money laundering and unlicensed check-cashing business case that evidence of the defendant's "wealth, spending, and lifestyle," including expenditures on, among other things, "luxury items…[and] renovations to [d]efendant's penthouse apartment" was "direct evidence of his committing the charged crimes, as well as his overarching motive for the criminal conduct") (quotation marks omitted))). Evidence of the defendant's concealment of his profits from the sale of his TORN tokens is also evidence of consciousness of guilt. (Dkt. 157 at 32). *See, e.g.*, *United States v. Silver*, 117 F. Supp. 3d 461, 473 (S.D.N.Y. 2015) ("Evidence that [the defendant] went to lengths to conceal his allegedly ill-gotten gains is evidence both of [his] knowledge that the money that he received constituted 'criminally derived property'… and evidence of [his] consciousness of guilt regarding his allegedly fraudulent and extortionate activities."); *United States v. Valenti*, 60 F.3d 941, 946 (2d Cir. 1995) (evidence that the defendant took several steps to hide his receipt of embezzled funds was "circumstantial evidence that [the defendant] knew that what he was doing was wrong"); *United States v. Hatfield*, 685 F. Supp. 2d 320, 327 (E.D.N.Y. 2010) (evidence that defendant moved funds out of the country was "more probative than prejudicial, as it tends to show [defendant's] consciousness of guilt").

The foregoing demonstrates that evidence of the defendant's profits is probative of the defendant's control of, and his motive and intent in operating, the Tornado Cash service and therefore should be admitted. In response, as to the money laundering and IEEPA charges in this case, the defendant offers only the unsupported assertion that "whether or not Mr. Storm made any profit from Tornado Cash is irrelevant and prejudicial." (Dkt. 155 at 16). But the degree to which a defendant profited from participating in a criminal scheme is highly probative of the defendant's

motive and intent to participate in the scheme, even aside from the particular relevance here of the defendant's design of the TORN tokens as part of his overall control and operation of the Tornado Cash service. *United States v. Salmonese*, 352 F.3d 608, 615 (2d Cir. 2003) ("[W]here a conspiracy's purpose is economic enrichment, the jointly undertaken scheme continues through the conspirators' receipt of their anticipated economic benefits.") (quotation marks omitted); *see also United States v. Samaria*, 239 F.3d 228, 235 (2d Cir. 2001) (receipt of profits from a conspiracy is evidence of participation therein).

As for the money transmitting business charge, the defendant repeats his argument from his motion to dismiss that proof of his profits from the Tornado Cash service is not relevant absent evidence that the service earned profits on a fee-per-transaction basis. (Dkt. 155 at 16-17). That argument is wrong on two counts. First, the Court already rejected that argument in denying the motion to dismiss, explaining that under Second Circuit precedent there is no "fee" requirement; rather, a "business" under Section 1960 is "an enterprise that is carried on for profit or financial gain." (Dkt. 99 at 24 (citing *Banki*, 685 F.3d at 114)). Second, even if there were a fee requirement, the defendant concedes that users of the relayer network were charged a fee. (Dkt. 155 at 19). As detailed in the Werlau disclosure, the Tornado Cash founders structured the service so that holders of TORN tokens—which includes the defendant—benefitted from those relayer fees. Thus, the defendant's argument seems to be that, not only must the Government prove that fees were charged, but it must also prove that the fees were paid directly to the defendant, rather than that the relayer fees were part of the overall profit-making nature of the business. That argument is both unsupported by any authority and lacking in any logic. One can make a profit on an enterprise—by selling appreciated stock, for example—without direct receipt of fee income. The same is true here; whether his earnings from TORN sales were themselves fees, they were profits

to him from his operation of the Tornado Cash service and they demonstrate the for-profit nature of the enterprise.

The defendant attempts to draw a distinction between his profits from selling TORN and the question whether the Tornado Cash service was operated for profit. (Dkt. 155 at 20). But at most, he has identified an issue for the jury as to whether the Tornado Cash service made a profit and how to define the constituent parts of the service. For example, the defendant excludes the operation of the relayer network and registry from his description of the parts of the Tornado Cash service that drew revenue from fees. (*Id.*). But that essentially assumes the conclusion, and the evidence will show that these features of the service were designed to be interconnected, and that the defendant exercised control over the relayer network as a means to earn profits. (Dkt. 157 at 31). This evidence goes directly to the elements of 18 U.S.C. § 1960(b)(1)(C), Thus, evidence of defendant's TORN-related profits is admissible because it is "a step on one evidentiary route to the ultimate fact." *Old Chief v. United States*, 519 U.S. 172, 179 (1997).

Ultimately, the defendant's motion rests on attempting to resolve disputed factual issues ahead of trial, as he asserts that his profits from selling TORN were not "associated with the usage of the Tornado Cash protocol," and that "the value of TORN plummeted during the post-relayer registry period." (Dkt. 155 at 18-19). But those issues are hotly disputed, as the Government alleges that TORN prices actually increased during this period (Indictment ¶ 71), and expects that the evidence at trial will show that TORN prices rose in response to the implementation of the relayer algorithm.

Moreover, whether TORN prices in fact increased is less relevant than the defendant's intent to profit by linking TORN tokens to the fees earned by the relayers, which is the legally salient point. There will be ample evidence (largely in the form of the defendant's own messages

with his co-founders and employees) that the defendant told his co-conspirators that they needed to "pump the price" of TORN, that he specifically explained his goal in implementing the February 2022 changes to connect TORN value to relayer fees, and that he then liquidated his substantial TORN holdings in the ensuing months. Thus, while the defense may attempt to argue to the jury that there was not a "direct pecuniary link" between the operation of the Tornado Cash service and the defendant's profits, the Government expects that the evidence will show that the defendant viewed them as connected. Ultimately, the defendant's arguments about what inferences to draw from this evidence do not in any way call into question its admissibility.

The defendant's arguments under Rule 403 are similarly unavailing. The Government has established a foundation for admitting the evidence of the defendant's profits and he has made no real attempt to show how the probative value of that evidence would be outweighed by any unfair prejudice. Fed. R. Evid. 403. *See also Costantino*, 203 F.3d at 174 ("Because virtually all evidence is prejudicial to one party or another, to justify exclusion under Rule 403 the prejudice must be unfair."); *United States v. Hoey*, 725 F. App'x 58, 61 (2d Cir. 2018) (evidence of defendant's spending habits was evidence of motive in an embezzlement, wire fraud, and money laundering case and was not more prejudicial than probative); *Motovich*, 2024 WL 3303723, at *2 (evidence of defendant's wealth, spending, and lifestyle "is probative of and relevant to the charged crimes [money laundering and unlicensed money transmitting business], and such probative value is not substantially outweighed by the danger of unfair prejudice).

V. Opposition to MIL No. 6: Evidence of the Defendant's Consciousness of Guilt is Admissible.

As set forth above, the defendant's sales of TORN and the complex set of transactions in which he engaged to conceal his profit taking is direct evidence of the charged conspiracies and/or intent and consciousness of guilt evidence admissible under Rule 404(b). (*See* Dkt. 157 at 31-32).

As part of that concealment, the defendant conducted cryptocurrency transactions using an account in the name of another person who happened to be a Russian national. (Dkt. 157 at 31-32; Indictment ¶¶ 73-75). The fact that the defendant used an account in another person's name, and used a VPN to make it appear that he was in that person's location, are not references at all to the defendant's personal background. On the contrary, the nationality of the account holder is evidence taken from the defendant's own statements regarding it, in which he stated that he, as translated from Russian, "did everything from the Russian Binance ... and even from a Russian IP (VPN)." (Indictment ¶ 73). This reference to the fact that the defendant was using what he referred to as a "Russian Binance" account is highly probative in that it corroborates other evidence showing that the defendant was using a particular Binance account that was in fact in the name of a Russian national, and it is far less prejudicial than the sort of evidence of a defendant's own statements that courts routinely admit. *See United States v. Pierce*, 785 F.3d 832, 841 (2d Cir. 2015) (deciding and citing cases holding that defendant's tattoos and rap lyrics were relevant to show motive and participation in a conspiracy and the probative value of the evidence was not outweighed by unfair prejudice). Like the other evidence regarding the defendant's TORN sales, this is direct evidence of the conspiracies and is also admissible as evidence of intent and consciousness of guilt.

The Government does not intend to make gratuitous references to the defendant's (or anyone else's) national origin, and it has not done so here. *See* Indictment ¶¶ 73-75 (quoting defendant's own statement about the "Russian Binance," but otherwise simply referring to it as the "Binance account"). The Government expects the Court will instruct the jury that any feelings about the national origin of the defendant or anyone else are irrelevant, as requested in the Government's request to charge. (Dkt. 156 at 69). But it is certainly not gratuitous or unfairly prejudicial for the Government to offer the defendant's own description of the concealment

transactions he effectuated. *See United States v. Dicosola*, No. 12 CR 446, 2016 WL 362388, at *4 (N.D. Ill. Jan. 29, 2016) ("Defendant's state of mind was at issue throughout trial. It was not improper, let alone unfairly prejudicial, for the Government to ask the Court to consider Defendant's own words when evaluating his state of mind.").

The evidence about the Binance account is directly tied up with why, when, and how the defendant sold his TORN and is therefore admissible for the reasons explained above. The defendant claims that admitting this evidence would "open up a flood of evidence regarding a possibly confusing collateral issue" (Dkt. 155 at 23), but does not identify what the collateral issue might be or explain why it might be confusing. Thus, he fails to meet Rule 403's standard for exclusion.

Likewise, the defendant's statements to his co-conspirators encouraging them to further conceal funds he distributed to them in April 2022 are powerful evidence of consciousness of guilt and of a piece with the other evidence related to the defendant's sales and distributions of TORN in this period. Taken together, this evidence is probative of the defendant's "guilt and all the circumstances surrounding the offense" and is admissible. *Old Chief*, 519 U.S. at 183. The defendant argues that there may have been "lawful and valid reasons" for him to advise his co-founders to conceal their proceeds (Dkt. 155 at 24), but those are arguments about what inferences to draw from this evidence, not arguments to exclude the evidence.

VI. Opposition to MIL No. 7: The Court Should Exclude Evidence that OFAC's Sanctions on the Tornado Cash Smart Contract Pools Were Held Unlawful and Should Allow References to OFAC's Imposition of those Sanctions.

The Court should exclude evidence that OFAC's sanctions on the immutable Tornado Cash smart contract pools were held unlawful in *Van Loon v. Dep't of the Treasury*, 122 F.4th 549 (5th Cir. 2024), because any such evidence is irrelevant. The *Van Loon* decision—which says nothing

about criminal liability under IEEPA or any other law—was announced more than two years after any time frame that is relevant to this case and cannot retroactively shed any light on the defendant's conduct or state of mind during the charged time period. And even if there were some relevance, it is substantially outweighed by the danger of unfair prejudice, confusing the issues, misleading the jury, undue delay, and wasting time, and thus should be precluded under Rule 403. By contrast, the Court should allow references to OFAC's imposition of those sanctions, which is necessary to explain highly probative evidence of how the defendant acted in the immediate aftermath of the announcement.

A. Evidence that OFAC's Sanctions on the Tornado Cash Smart Contract Pools Were Held Unlawful Is Irrelevant and Highly Prejudicial.

Van Loon has no bearing on this case. (*See* Dkt. 120 at 1-2). The Fifth Circuit's reasoning rests on a factual conclusion that the Government not only does not dispute, but has affirmatively alleged in the Indictment: the smart contract pools were immutable, and therefore outside the defendant's control. (*See* Indictment, Dkt. 1 ("Ind.") ¶ 26)). The defendant has moved three times for the case to be dismissed based on his purported lack of control over the smart contracts. (*See* Second Mot. to Dismiss, Dkt. 164 ("MTD 2"); Mot. for Recons., Dkt. 112 ("MFR"); Mot. to Dismiss, Dkt. 30 ("MTD")). The Court rejected the first two motions to dismiss, concluding in its Order denying the second motion that *Van Loon* is not relevant, and should do the same with respect to the third. (*See* Denial of MFR, Dkt. 127 at 1-2 ("The Court does not believe [the money laundering and money transmitting charges] are impacted by the reasoning of *Van Loon*," and "*Van Loon* does not require dismissal [of the sanctions evasion charge] because it does not bear on the charged conduct"); Denial of MTD, Dkt. 99). Indeed, there will be no dispute at trial that the defendant gave up control of the smart contract pools in 2020. Rather, the dispute will be

whether the defendant committed crimes in the course of continuing to actively operate the integrated whole of the various interconnected components of the Tornado Cash service that he helped design and maintain. *Van Loon*, which concerned only the question whether OFAC could impose sanctions on the "immutable" smart contract pools, is simply immaterial to that dispute and therefore has no probative value to the defense. *See Van Loon*, 122 F.4th at 565 (explaining that only the "smart contracts that are *immutable*"—i.e., the pools—are "at issue in this appeal") (emphasis in original).

In addition to being irrelevant, any mention of *Van Loon* would be highly prejudicial to the Government. The defendant's arguments reveal that he would impermissibly seek to suggest to the jury that the Fifth Circuit's invalidation of OFAC's sanctions on the immutable smart contract pools somehow negates any potential criminal liability here with respect to his operation of the Tornado Cash service. That is a *non sequitur*, but it nonetheless carries a sort of false logic—and it is precisely the erroneous conclusion that the defendant invites the Court (and by extension the jury) to reach in his most recent motion to dismiss: "As the Fifth Circuit held in *Van Loon*, the lack of control over the smart contracts rendered civil sanctions invalid. If civil sanctions cannot be imposed on Tornado Cash, then certainly criminal liability cannot be imposed on Mr. Storm." (MTD 2 at 7 (citation omitted)). The defendant is comparing apples and oranges. *Van Loon* was decided on an administrative record and was narrowly focused on whether an immutable smart contract—standing alone, and without reference to anything else that contract might be connected to—is property that can be owned and therefore sanctioned. This case will involve a broader trial record, it will ask the jury to apply that record to a set of *criminal* laws that were not at issue in *Van Loon*, and in no way implicates whether an immutable smart contract is "property" under IEEPA that can be sanctioned. The defendant's intention here is plain: he wishes to mislead and

confuse the jury into thinking that *Van Loon* supports an acquittal, when it does nothing of the sort. And, given the distinctions between the legal question and factual record at issue in *Van Loon* and this case, all of which would need to be explained to the jury, it is highly probable that introduction of *Van Loon* would confuse the jury and lead them to the erroneous determination that *Van Loon* compels a verdict of not guilty here. That is exactly what Rule 403 is designed to prevent. Accordingly, the Court should exclude any evidence of *Van Loon* or any other indication that the smart contract pool sanctions were held unlawful or withdrawn by OFAC.

B. References to OFAC's Imposition of Sanctions on Tornado Cash Are Necessary to Explain Highly Probative Evidence.

By contrast, limited reference to the fact that OFAC imposed sanctions on Tornado Cash are necessary because they provide critical context for subsequent acts and statements of the defendant and his co-conspirators that are highly probative. Specifically, after sanctions were imposed on August 8, 2022, the defendant and his co-conspirators, among other things: (i) took steps to transfer control of the Tornado Cash Ethereum domain, which was the means by which they controlled the user interface, from themselves to the Tornado Cash DAO; (ii) expressed concern that third-party service providers who the defendants had been paying to facilitate the operation of the Tornado Cash service were dropping them in order to comply with sanctions; and (iii) liquidated large quantities of TORN while taking care to cover their tracks. These acts are compelling evidence that key features of the Tornado Cash service were controlled by the defendant and his co-founders, and that much of the "decentralization" on which the defendant relies only occurred when he deliberately took steps to decentralize the service after it was sanctioned. They also are key to understanding that the defendant both expected to profit from operating the Tornado Cash service, and did in fact profit by cashing out for millions of dollars in

August 2022. They also establish the defendant's consciousness of guilt regarding the charged offenses. But these acts are impossible to understand without reference to the imposition of sanctions that prompted them, which, accordingly, should be permitted. Any prejudice resulting from such references is far outweighed by their probative value and, in any event, would be entirely mitigated by a curative jury instruction. And, indeed, the Government does not intend to prove up the Tornado Cash sanctions beyond the following, none of which is inflammatory.

On the day sanctions were imposed, August 8, 2022—which is the last day of the charged timeframe in the Superseding Indictment—the Tornado Cash founders circulated among themselves the Treasury Department's press release announcing the smart contract pool sanctions and news articles reporting on the announcement.[9] On that day, shortly after learning of the sanctions, the founders transferred ownership and control of the tornadocash.eth domain (the internet address where the Tornado Cash service's customers could access the UI) to the Tornado Cash governance smart contract. Before the transfer, the domain was entirely under the control of the three founders, using an Ethereum address associated with Semenov. After the transfer, it was entirely under the control of the Tornado Cash DAO. This strongly undermines the defendant's claim that the Tornado Cash service was controlled by the DAO, rather than the defendant and his co-conspirators, during the charged time period. Indeed, it demonstrates that the defendant and his co-conspirators did not begin to transfer control of key components of the Tornado Cash service

[9] *See Cyber-related Designation*, Office of Foreign Assets Control (Aug. 8, 2022), https://ofac.treasury.gov/recent-actions/20220808; Jerry Brito and Peter Van Valkenburgh, *U.S. Treasury sanction of privacy tools places sweeping restrictions on all Americans* (Aug. 8, 2022), https://www.coincenter.org/u-s-treasury-sanction-of-privacy-tools-places-sweeping-restrictions-on-all-americans/; David Hollerith and Jennifer Schonberger, *U.S. sanctions crypto mixing service Tornado Cash, citing North Korea ties* (Aug. 8, 2022), https://finance.yahoo.com/news/tornado-cash-treasury-sanctions-north-korea-145228318.html?guccounter=1.

to the DAO until the end of the charged time period, immediately after sanctions were imposed, in order to distance themselves from the enterprise because they knew that law enforcement would be scrutinizing their past actions due to the sanctions. Accordingly, this evidence is highly probative of the defendant's control of the Tornado Cash service during the charged time period—which the defendant will hotly contest at trial—and his consciousness of guilt regarding the charged offenses.

On August 9, 2022, the day after sanctions were imposed, Alchemy—a third-party service provider that the defendant contracted with to facilitate traffic between the UI and the Ethereum blockchain—dropped the defendant and his co-conspirators as customers. The defendant expressed anger that Alchemy had taken this law-abiding step, concern that other service providers he was paying would follow suit, and alarm that Alchemy's decision would disable the UI and relayer registry. "Alchemy dropped us," he wrote to his co-conspirators (as translated from Russian), followed in quick succession by "Infura is next" (referring to another service provider), and "*ui* is fucked" (referring to the UI's inability to operate without these service providers). Within an hour, the defendant observed, as translated from Russian, "The relayer registry is fucked because of Alchemy," and, "It's quite possible the [*sic*] Infura is going to fuck us now too." These events and statements establish that the defendant and his co-conspirators operated the Tornado Cash service in part by contracting with critical service providers, who they viewed as vital to the operability of the Tornado Cash service during the charged time period. It is also direct evidence that the defendant considered the various components of the Tornado Cash service working together as a whole, *i.e.*, not just the smart contracts, which will be a hotly contested issue at trial. Like the transfer of the tornadocash.eth domain, this evidence directly refutes the defendant's claim that he and his co-conspirators were not exercising control over and paying operational costs

for the Tornado Cash service during the charged timeframe. Accordingly, this evidence is highly probative.

Also probative is evidence that the defendant liquidated millions of dollars' worth of TORN after the imposition of sanctions and that he attempted to cover his tracks in doing so. Specifically, within minutes of seeing press coverage of the imposition of sanctions, the defendant began aggressively converting TORN tokens into more than 12 million dollars' worth of other cryptocurrencies using the Binance account referenced above that was in the name of another person. He then transferred approximately 8 million dollars' worth of those assets, via a cryptocurrency address in his control, to three cryptocurrency addresses where he and his two co-conspirators could access their respective shares of the funds. That the defendant liquidated a large quantity of TORN after the imposition of sanctions via numerous cryptocurrency addresses and an exchange account belonging to someone other than him and his co-conspirators establishes two important points. First, the defendant believed that the price of TORN would fall as a result of the smart contract pool sanctions' negative effect on smart contract activity. This evidence tends to refute the defendant's claim that the price of TORN was unaffected by smart contract activity and to prove that TORN was in fact the economic engine and profit center of the Tornado Cash service. It also tends to prove that the defendant cared about the value of TORN and that he perceived that his payday from Tornado Cash was under threat, as he liquidated such large quantities at the same time that he transferred control over operational aspects of the service to the DAO.

Second, this evidence is probative of consciousness of guilt, as the defendant sought to cover his tracks in how he held and liquidated TORN tokens in a cryptocurrency account in another person's name, which evidences that he knew he had committed the charged offenses and suspected that—especially in the wake of the imposition of sanctions on the smart contract pools—

law enforcement would scrutinize his actions and possibly seize his ill-gotten gains. Indeed, the defendant sent messages to his co-founders advising them to take further steps to conceal the proceeds by creating new wallets and transferring the money to new addresses. (Indictment ¶ 75). The Government should be permitted to present this highly probative evidence, and the fact that it all took place in the immediate aftermath of sanctions is necessary context for explaining it.

There is no basis to exclude references to the imposition of sanctions on the smart contract pools under Rule 403. As set forth above, such references have significant probative value in demonstrating the defendant and his co-conspirators' control of the Tornado Cash service during the charged timeframe and his consciousness of guilt. As noted above, references to OFAC's sanctions on the Tornado Cash pools will be limited to the dry testimony of the OFAC representative about the existence of the sanctions and the defendant and his co-conspirators' own statements about the sanctions. None of this is "more sensational or disturbing" than the charged offense, and any prejudice resulting from such references is minimal and outweighed by their probative value. *See United States v. Roldan-Zapata*, 916 F.2d 795, 804 (2d Cir. 1990); *United States v. Taylor*, 767 F. Supp. 2d 428, 438 (S.D.N.Y. 2010). Any prejudicial effect, moreover, could be further reduced by a limiting instruction, and the Government does not object to such an instruction explaining that the defendant is not on trial for violating the sanctions imposed in August 2022 and that evidence of those sanctions is being offered for the limited purposes described above. *Huddleston v. United States*, 485 U.S. 681, 691-92 (1988).

VII. Opposition to MIL No. 8: The Government Does Not Intend to Argue that Anonymous Blockchain Activity or Crypto-Mixing Is Inherently Illicit.

MIL No. 8 should be denied as moot because the Government does not intend to argue "that crypto-mixing protocols, or anonymizing protocols more generally, are inherently suspicious or constitute illicit activity." (Dkt. 155 at 27). MIL No. 8 should also be denied to the extent that

it seeks to preclude the Government from arguing that the crypto-mixing protocol at issue here, the Tornado Cash service, *could be* and, in fact, *was* used for suspicious or illicit activity, as this obviously goes to the heart of the Government's case. *United States v. Guo* is not to the contrary. No. 23 CR. 118 (AT), 2024 WL 2262706, at *4 (S.D.N.Y. May 17, 2024), *on reconsideration in part*, 2024 WL 3104538 (S.D.N.Y. June 24, 2024), There, Judge Torres permitted the Government's expert witness, "in explaining why [he] considers certain features of cryptocurrencies to be important,…[to] mention[cryptocurrency's] potential for misuse, theft, or fraud." *Id*. The Government's expert in *Guo* was only prohibited from testifying about cryptocurrency frauds that had no relation to the charged crimes. Here, the Government's intention is to keep the focus squarely on the Tornado Cash service, as opposed to, say, the defendant's stated desire to elicit expert testimony on, among other things, "the importance of online privacy," various online tools relating to privacy, the legality of certain types of privacy tools, and what actors in the cryptocurrency industry generally intend regarding criminal activity. (Dkt. 159, Ex. 1A, Defense Expert Disclosure, Dr. Matthew Green).

VIII. Opposition to MIL No. 9: The Court Should Deny the Defendant's Motion to Preclude the Government and its Witnesses from Referring to the Tornado Cash Service and Its Customers as Anything other than "Tornado Cash" and "Users"

The Government and its witnesses should be permitted to refer to the Tornado Cash "service," and to its users as "customers," because those are accurate, plain-English descriptions of Tornado Cash and those who used it, supported by overwhelming evidence that the Government will present at trial—and because those terms are necessary to complete the story of the defendant's crimes.

First, as a factual matter, the evidence at trial will show that Tornado Cash did in fact provide a service to paying customers. It was a for-profit organization that provided

cryptocurrency concealment and transmission services to depositors, the vast majority of whom paid fees to relayers, which, in turn, were required, in effect, to direct a portion of those fees to the Tornado Cash service's governance contract in order to be selected to process the transactions. Indeed, while the Lazarus Group was laundering the Ronin Hack proceeds through the Tornado Cash service, the defendant circulated to his co-conspirators a news article that described Tornado Cash as a "service."[10] And he received email correspondence about particular hacks that described Tornado Cash as a "service." (Ex. B). Indeed, abundant evidence will establish that this description is accurate and that the Tornado Cash service had paying customers. The evidence will include: testimony from an expert who has studied the Tornado Cash service's underlying code; numerous statements by the defendant and his co-conspirators revealing their intent—and the actions they took—to generate profits in exchange for providing cryptocurrency concealment services; and tracing analysis showing that the defendant and his co-conspirators reaped millions of dollars' worth of profits by operating the Tornado Cash service.

At bottom, restricting use of the terms "service" and "customer" at trial would curtail the Government and its witnesses' ability to describe the organization at the center of this case for what it is, and Courts routinely permit far more prejudicial language to describe organizations, charged conduct, and defendants themselves when necessary to complete the story of a crime. *See, e.g.*, *United States v. Giovinco*, 382 F. Supp. 3d 295, 298 (S.D.N.Y. 2019) ("The Court is not persuaded that references to 'La Cosa Nostra,' the 'Mafia,' and the 'Genovese Crime Family' would unfairly prejudice Giovinco."); *United States v. Malka*, 602 F. Supp. 3d 510, 554 (S.D.N.Y.

[10] *See* Danny Nelson, *Sanctioned Crypto Wallet Linked to North Korean Hackers Keeps Laundering*, CoinDesk (April 15, 2022), https://www.coindesk.com/tech/2022/04/15/sanctioned-crypto-wallet-linked-to-north-korean-hackers-keeps-on-laundering.

2022) (permitting the Government to use the terms "kidnapping" and "abduction" in a kidnapping case); *United States v. Ahmed*, 94 F. Supp. 3d 394, 436 (E.D.N.Y. 2015) (rejecting the defendant's motion to preclude Government usage of terms relating to terrorism and finding "no basis to preclude the Government from using words that are central to the case").[11]

The case law cited by the defendant on this issue is simply inapposite. (*See* Def. MIL No. 9 at 31, 43). In *United States v. Scop*, the Second Circuit found that the district court had erred in allowing a Government expert to use terminology that "drew directly upon the language of the statute and accompanying regulations concerning 'manipulation' and 'fraud,'" thereby expressing "legal conclusions that were highly prejudicial." 846 F.2d 135, 140 (2d Cir. 1988). The same is true of *Highland Cap. Mgmt., L.P. v. Schneider*, where the court found the terms "'securities fraud,' 'illegal,' 'insider trading,' 'inside information,' and 'market manipulation'" overly prejudicial. 551 F. Supp. 2d 173, 193 (S.D.N.Y. 2008). By contrast, the everyday terms "service" and "customer" do not draw on the language of any of the statutes at issue in this case. Moreover, the Circuit observed in *Scop* that the terms "'manipulation,' 'scheme to defraud,' and 'fraud' are not self-defining terms but rather have been the subject of diverse judicial interpretations." 846 F.2d 135 at 140. Conversely, the terms "service" and "customer" are straightforward, commonplace, and not subject to legal or industry exegesis.[12] Lastly, in *United States v. Patel*, the

[11] The Government notes that the defendant's filings in this case repeatedly refer to the Tornado Cash service as a "protocol," a less straightforward and commonly-used term than "service," apparently meant to imply distance between the defendant and the cryptocurrency mixing services provided by Tornado Cash. (*See, e.g.*, Def. MILs at 10, 15, 18, 20, 22-26, 34, 36, 40). Rather than seek a gag order on the use of that ambiguous term, the Government recognizes that how Tornado Cash is characterized—and the relevance of that characterization to the elements of the charged offenses—is ultimately a matter for the jury to decide on the basis of the facts proven at trial.

[12] Indeed, the defendant appears to concede that the term "customer" is uncomplicated, defining it simply as "a person who buys goods or services." (Def. MIL No. 9 at 33).

defendant, Mahesh Patel, was charged with one count of conspiracy in restraint of trade, in violation of the Sherman Act, for participating in an agreement among various companies to restrict hiring and recruiting practices in certain ways. No. 3:21-CR-220 (VAB), 2023 WL 2643815, at *1 (D. Conn. Mar. 27, 2023). The Court found more prejudicial than probative the term, "Mahesh Patel Rule," which had been used—by just one of multiple co-conspirators, for only a limited time—to describe the anticompetitive hiring and recruiting agreement at the center of the alleged conspiracy. *Id.* at *11-12. In other words, the court found overly prejudicial a term that literally named the criminal scheme after the defendant. The terms "service" and "customer" are utterly unobjectionable by comparison. In sum, "service" and "customer" are straightforward, commonplace words that accurately describe Tornado Cash and its users based on ample evidence, and there is no basis to restrict their use at trial.

IX. Opposition to MIL No. 10: The Court Should Deny the Defendant's Motion to Preclude Summary Charts and Testimony and His Motion for Advance Disclosure of Summary Charts.

The defendant speculates at length that the Government might offer improper summary charts or testimony. (*See* Def. MIL No. 10 at 35-40). He is mistaken, as any summary charts or summary testimony offered by the Government will comport with the Rules of Evidence. In any event, the deadline for production of exhibits (including summary charts) and 3500 material (which, in turn, will result in the identification of witnesses) has not yet come to pass. Accordingly, there is no basis for the defendant's conjecture that preclusion of any summary charts or summary testimony—or "thorough cross-examination" of summary witnesses—will be warranted, and the Court should deny the defendant's motion for these forms of relief as unripe. (*Id.* at 40).

Nor should the Court grant the defendant's motion for advance disclosure of summary charts, which also lacks any basis except that summary charts have been found improper in other

cases—which, obviously, does not warrant any relief in this case. The Government will produce summary charts with the rest of its exhibits on the deadline the Court has set, which will leave ample time for the defendant to make any objections before trial.

CONCLUSION

For the reasons set forth above, the Court should deny each of the Defendant's motions *in limine*.

Respectfully submitted,

JAY CLAYTON
United States Attorney for the
Southern District of New York

By: /s/ Thane Rehn
Ben Arad
Benjamin A. Gianforti
Thane Rehn
Assistant United States Attorneys

Kevin Mosley
Special Assistant United States Attorney
(212) 637-2354

Dated: June 18, 2025
New York, New York